TRUCE

A Guide to Creating an Effective Mobile Device Usage Policy

Nearly 9 out of 10 businesses today rely on their employee's ability to access mobile business applications from their mobile devices[1]. Most organizations will choose to use either Company-Provided or Bring-Your-Own-Device programs (or a combination of the two) to enable the mobile productivity of their workforce. And so it becomes all the more important to keep those devices useful and secure while also protecting the safety of the employees. So why is it that less than half of decision-makers believe their current mobile policies meet today's safety or productivity needs[2]?

Creating a mobile policy should not be done in a vacuum. By working with the various stakeholders across your organization to understand how and when a mobile device is required, and what guidelines they'd like to see established, you can create a more robust policy that accommodates how people actually work at your organization. Involving employees in the process may not be top of mind but could give you the added benefit of compliance once the policy is rolled out.

Below are some additional tips on creating and implementing an effective mobile device policy:

View your policy as a way to formalize your business strategy.

Why does your company rely on mobile devices to get work done? How and when should your employees be using them? What circumstances or environments require tighter or looser management over device usage? It's important to be as specific as possible in the policy so that everyone reading it understands how the right use of mobile devices impacts the business and the individuals in meeting their goals.

Elements of an Effective Mobile Device Policy

Company policies can vary when it comes to length and complexity – everything from high-level do's and don'ts to page after page of detailed discussion around acceptable use. Whatever the style for your company, the following components of an effective policy should be incorporated into the final document:

1. Scope
What constitutes a mobile device as it relates to the policy? Will the policy cover just corporate-issued devices and bring-your-own-devices, or does it also cover personal phones brought on site for personal use? Establish this right up front so everyone understands what's in and what's out.

2. Business Requirements
How are mobile devices used at the workplace? Why are they critical to business operations? Are there specific roles that have a higher need for mobile access? Use this section to clarify the business strategy behind the use of mobile devices at your organization.

Define the steps needed to secure both the device and your network.

Ensuring safe and secure access to your network and proprietary data is the responsibility of both the company and the employee. Make sure your policy defines both the employee and company obligations. And be clear in what those obligations are, whether its specifying the complexity of passwords, to requiring employees to deploy antivirus, anti-spyware or device management software on personal devices or detailing a checklist of security upgrades an employee-owned device needs to pass before it can be used for work.

Be consistent in the implementation of the policy.

No policy is worth implementing if individual employees are able to use different standards to dictate their work habits, or worse, can choose whether or not to follow the rules. Define how the policy will be rolled out and how you will audit compliance over time.

Educate your employees and keep awareness high.

An effective policy addresses the needs of the entire organization, from top-level executives, to management and frontline workers as all employees are impacted by how and when mobiles devices are used in the workplace. When done right, the policy is not viewed as something “done to the employee” but as a platform for everyone to support in order to protect what’s most important – employee safety and the integrity of the company’s network and proprietary data. Make sure employees are educated on not just the terms of the policy but the “why’s” behind it by offering insights on industry and your own organization’s safety trends, cybersecurity trends and productivity trends.

Lastly, find the right person to write the policy.

Whether the policy is drafted by the IT department, the Health & Safety department or the Operations department, it should be written in clear, easy to understand language to ensure the highest compliance. After all, the easier it is to understand the rules, the more likely someone is to follow them.

Sources

1. https://syntonic.com/wp-content/uploads/2016/09/Syntonic-2016-BYOD-Usage-in-the-Enterprise.pdf
2. Unleash the Full Potential of Mobile with Contextual Mobile Device Management, a Forrester Consulting Thought Leadership Paper commissioned by TRUCE Software, August 2019

To learn more, go to **www.trucesoftware.com**.

TRUCE

3. Employee Obligations

Make sure your policy details what is considered appropriate use and be specific about the use of apps and features in different situations. What may be appropriate use in a break room is probably not acceptable on a production floor. Be sure to also include the Employee’s responsibility when it comes to the security of the device. What are your requirements for passwords? Is there a security checklist they need to follow if they want to bring their own device on site and access company networks? It’s common in any policy for there to be a user requirement to install security software on the personal device. Establishing the right guidelines can make it easier for employees to understand and thus comply with the policy.

And don’t forget to explain what disciplinary action will be taken for non-compliance. The policy is there for a reason and everyone needs to understand it’s not optional.

4. Company Obligations

Following the employee obligations, it’s important to show the other side of the equation, namely what your company will be doing to support the policy. If you have a BYOD program, state what the approval process (if any) looks like along with any reimbursement commitments. What tools are you implementing, such as endpoint management software or CMDM platforms, to ensure the safe and secure use of mobile devices at the workplace?

5. Signature

Make sure your employees acknowledge not only that they have read and understood the policy, but that they agree to the terms set by that policy. With the company representative’s signature, you’re acknowledging the importance mobile devices have in the workplace.